UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/685,119 | 10/14/2003 | Carl A. Bender | POU920030206US1 | 4468 |

7590 09/22/2006

Lawrence D. Cutter, Attorney
IBM Corporation
Intellectual Property Law Dept.
2455 South Rd., M/S P386
Poughkeepsie, NY 12601

| EXAMINER | |
|---|---|
| TRUONG, LOAN | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2114 | |

DATE MAILED: 09/22/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/685,119 | BENDER ET AL. | |
| | Examiner | Art Unit | |
| | LOAN TRUONG | 2114 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *7/14/2006*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *2-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *2-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *14 October 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

1. This Office Action is in response to the amendment filed July 14, 2006 in application 10/685,119.

2. Claims 2-21 are presented for examination with claims 2-21 newly added.

### *Response to Arguments*

3. Applicant's arguments with respect to claim 1 have been considered. Claims 2-21 are presented in view of the new ground(s) of rejection.

### *Claim Rejections - 35 USC § 102*

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 2-21 are rejected under 35 U.S.C. 102(b) as being anticipated by Burrows et al. (US 2002/0073338).

In regard to claim 2, Burrows et al. disclosed a method of providing data integrity in a data processing system which transfers message packets from a plurality of nodes through communication adapters, said method comprising the steps of:

Monitoring adapter activity to detect corruption of any message packet to be transferred by any adapter (*monitor the network for any pattern of packet traffic behavior that can be considered undesirable, paragraph 0030 lines 4-6)*;

Providing an interrogatable internal storage area (*tables contain an entry for each network that can be reach from the router, paragraph 0034 lines 6-11, packet traffic monitor can poll or interrogate that information in gaining its understanding of the network topology, paragraph 0034 lines 20-22)* for each adapter for storage of pertinent error detection and recovery data in case of data corruption (*understanding network topology helps in deciding which port should be disabled when undesirable packet is detected, paragraph 0033 lines 2-5)*;

Once an error that can potentially cause data corruption of any message packet is detected, temporarily making said adapter unavailable to any node(s) in said system until corrupted message packet is cleared (*preferred way of influencing the forwarding scheme is filtering source MAC addresses to isolate a particular offending host or segment for a certain time periods, paragraph 0043 lines 14-17).*

In regard claim 3, Burrows et al. disclosed the method of claim 2, further comprising the step of determining if data corruption of said message packet is transferred beyond said adapter to said system (*packet traffic monitor, fig. 2-4)*

In regard to claim 4, Burrows et al. disclosed the method of claim 3, wherein said system is cleared of said data corruption by causing a system check stop (*skeptic enters a wait state before it lets such component or connectivity to recover, paragraph 0045).*

In regard to claim 5, Burrows et al. disclosed the method of claim 4, wherein said system is then reinitialized and reset (*rejoin the network sand prompt reconfiguration of the network topology, paragraph 0045).*

In regard to claim 6, Burrows et al. disclosed the method of claim 5, wherein said adapter is temporarily made available by fencing said adapter off from said system and to said associated nodes (*packet traffic monitor can cause an offending host to be isolated from the network, paragraph 0046).*

In regard to claim 7, Burrows et al. disclosed the method of claim 5, wherein said adapter is then reset (*a component is taken out of operation for successively longer periods in a random exponential backoff before an attempt is made to use it once more, paragraph 0045).*

In regard to claim 8, the method of claim 7, wherein said adapter can differentiate between different levels of data corruption severity (*packet traffic monitor will isolate the faulty host for exponentially increasing time periods while the undesirable behavior continues or repeats, paragraph 0047).*

In regard to claim 9, Burrows et al. disclosed the method of claim 8, wherein said adapter is temporarily removed when said level of severity is deemed adequately high (*skepticism level, paragraph 0045).*

In regard to claim 10, Burrows et al. disclosed the method of claim 9, wherein each adapter is provided with an internal memory (*store routing table that contain an entry for each network that can be reached from the router, paragraph 0034).*

In regard to claim 11, Burrows et al. disclosed the method of claim 10, wherein information concerning corruption of message packets is then stored in a table within each adapter's internal memory (*broken component with a long history of failure, paragraph 0045).*

In regard to claim 12, Burrows et al. disclosed the method of claim 11, wherein said information to be stored also includes adapter state information (*skepticism level, paragraph 0045).*

In regard to claim 13, Burrows et al. disclosed the method of claim 12, wherein said adapter is also reinitialized before it is started and made available to said system (*rejoin the network sand prompt reconfiguration of the network topology, paragraph 0045).*

In regard to claim 14, Burrows et al. disclosed the method of claim 13, wherein said communication adapters are provided on each end of a switched link that are connected to said plurality of respective data processing nodes (*each host is self-policing with its dedicated packet traffic monitor, fig. 4, paragraph 0066)).*

In regard to claim 15, Burrows et al. disclosed the method of claim 14, further comprising the step of interrogating said adapter table from any node to which said adapter is connected (*tables contain an entry for each network that can be reach from the router, paragraph 0034 lines 6-11, packet traffic monitor can poll or interrogate that information in gaining its understanding of the network topology, paragraph 0034 lines 20-22)* to determine previous problems and errors logged (*broken component with a long history of failure, paragraph 0045).*

In regard to claim 16, Burrows et al. disclosed the method of claim 15, wherein said information is stored prior to resetting and reinitializing of said adapter (*rejoin the network sand prompt reconfiguration of the network topology, paragraph 0045).*

In regard to claim 17, Burrows et al. disclosed a method of data recovery and error detection in a data processing system having a plurality of nodes comprising:

Connecting one or more communication adapters to each end of any switched link such that said adapters can transfer message packets between said nodes (*switch-based network with packet traffic monitor, fig. 2-4)*;

Providing an interrogatable internal storage area (*tables contain an entry for each network that can be reach from the router, paragraph 0034 lines 6-11, packet traffic monitor can poll or interrogate that information in gaining its understanding of the network topology, paragraph 0034 lines 20-22)* for each adapter for storage of pertinent error detection and recovery data in case of data corruption (*understanding network topology helps in deciding which port should be disabled when undesirable packet is detected, paragraph 0033 lines 2-5)*;

Monitoring data transmission activity to detect data corruption of any of said message packets being transferred by said adapters (*monitor the network for any pattern of packet traffic behavior that can be considered undesirable, paragraph 0030 lines 4-6)*; and

Once data corruption is detected, temporarily removing said adapter availability from said nodes in said system (*preferred way of influencing the forwarding scheme is filtering source MAC addresses to isolate a particular offending host or segment for a certain time periods, paragraph 0043 lines 14-17)* until said adapter can be reset and reinitialized (*rejoin the network sand prompt reconfiguration of the network topology, paragraph 0045)* as to remove corrupted data and avoid such data to be transferred to other areas of said system (*influencing the forwarding scheme, paragraph 0043)*

In regard to claim 18, Burrows et al. disclosed the method of claim 17, wherein said adapter is capable of receiving and processing a wide range of commands and instructions to effectuate a plurality of different message packet transfer modalities (*packet traffic monitor is configured or programmed to recognize undesirable packet traffic patterns and to instruct appropriate switches to discard packets or isolate offending hosts, paragraph 0018).*

In regard to claim 19, Burrows et al. disclosed the method of claim 19, wherein information about said data corruption is provided in said internal storage area of said associated adapter prior to reinitializing of said adapter (*rejoin the network sand prompt reconfiguration of the network topology, paragraph 0045).*

In regard to claim 20, Burrows et al. disclosed the method of claim 19, further comprising the step of determining of said data corruption was transferred to said system and thereafter check stopping (*skeptic enters a wait state before it lets such component or connectivity to recover, paragraph 0045)* and reinitializing said system (*rejoin the networks and prompt reconfiguration of the network topology, paragraph 0045)* if said corrupted data was transferred by any adapters to said system (*addressing performance anomalies by influencing forwarding scheme in the switches, paragraph 0043).*

In regard to claim 21, Burrows et al. disclosed a data processing system comprising:

A plurality of nodes in processing communication with one another through a plurality of communication adapters connected to each end of switched links associated with said nodes such that data packets can be transferred between said nodes (*switch-based network with packet traffic monitor, fig. 2-4)*

Said communication adapters having an interrogatable internal storage area (*tables contain an entry for each network that can be reach from the router, paragraph 0034 lines 6-11, packet traffic monitor can poll or interrogate that information in gaining its understanding of the network topology, paragraph 0034 lines 20-22)* for storing pertinent error detection and recovery data in case of data corruption (*understanding network topology helps in deciding which port should be disabled when undesirable packet is detected, paragraph 0033 lines 2-5)*;

Said adapters capable of receiving and processing a wide range of commands and instructions to effectuate a plurality of different message packet transfer modalities (*packet*

*traffic monitor is configured or programmed to recognize undesirable packet traffic patterns and to instruct appropriate switches to discard packets or isolate offending hosts, paragraph 0018)*;

Means for detecting data corruption of packets and for temporarily making said adapters unavailable (*preferred way of influencing the forwarding scheme is filtering source MAC addresses to isolate a particular offending host or segment for a certain time periods, paragraph 0043 lines 14-17)* until information about said error can be stored in said adapters internal storage and said adapter can be reinitialized (*rejoin the network sand prompt reconfiguration of the network topology, paragraph 0045).*

***Conclusion***

*5.* The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. See PTO 892.

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LOAN TRUONG whose telephone number is (571) 272-2572. The examiner can normally be reached on M-F from 8am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, SCOTT BADERMAN can be reached on (571) 272-3644. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Loan Truong
Patent Examiner
Art Unit: 2114

SCOTT BADERMAN
SUPERVISORY PATENT EXAMINER